生成式AI跑得太快 各国监管机构迎头赶上

本报记者 曲忠芳 李正豪 北京报道

生成式AI持续火热发展的同时，在信息安全、数据合规、版权保护等方面也引发了社会的关注与热议。为促进生成式人工智能技术健康发展和规范应用，4月11日，国家互联网信息办公室（以下简称“网信办”）起草了《生成式人工智能服务管理办法（征求意见稿）》（以下简称《办法》），并向社会公开征求意见，意见反馈的截止时间为5月10日。

《中国经营报》记者注意到，《办法》共二十一条，明确了生成式AI应遵循的合规要求。简要概括来说：第一，《办法》划定了适用范围、对生成式AI给出了权威解释，鼓励行业开展基础技术自主创新、国际合作；第二是明确了权责划分和责任主体，重点强化了个人信息保护的相关要求，明确个人信息处理者的法定责任和义务；第三要求生成式AI产品或服务建立评估备案、实名制、投诉处理等机制，丰富了包括人工标注、防沉迷、内容标识等管理措施；第四则是规定了相应的整改及处罚措施。

“《办法》内容非常简洁明了，对生成式AI的一些热点问题进行了规范，预示着我国对于生成式AI的第一份政府文件或将出炉，在监管规范方面，我国走在了全球的前列。”浙江大学国际联合商学院数字经济与金融创新研究中心联席主任、研究员盘和林如是评价。

上海申伦律师事务所律师夏海龙指出，类似《办法》类监管文件的性质属于“部门规章”，根据相关规定，规章出台一般要经过立项、起草、审查、决定、公布等几个程序，在起草和审查阶段，往往需要向社会公开征求意见。

与此同时，本报记者从多位企业内部人士了解到，生成式AI产品服务提供商已关注到《办法》的公布，尤其是着重研究提供者对于生成式AI承担的责任义务方面。业内人士普遍认为，监管层面对生成工AI进行规范，将进一步抬高企业安全合规的门槛，增加相关成本。

监管风向：技术发展与安全合规同步推动

“《办法》体现了监管部门对生成式AI的一个有限范围的小心求证过程，保障在还不清楚生成式AI的各种可能性之前，各方安全可控地进行研发。”

记者注意到，近半个月以来，就ChatGPT引发的生成式AI热潮，全球多个国家的监管部门公开发声或表态，对其带来的数据安全等风险密切关注，并实施或者酝酿监管举措。就在3月31日，意大利数据保护局宣布暂时禁用ChatGPT并对该工具涉嫌违反隐私规则展开调查。不久，德国、西班牙等国的数据保护机构表态“不排除暂停ChatGPT使用的可能”。4月4日，加拿大隐私专员办公室宣布针对一项“未经同意收集、使用和披露个人信息”的投诉，开始对研发ChatGPT的OpenAI公司展开调查。4月11日，据《华尔街日报》报道，美国政府已经开始研究是否需要对ChatGPT等AI工具进行检查。

夏海龙指出，从《办法》内容来看，目前网信办的监管路径相对比较清晰，即以《网络安全法》《数据安全法》和《个人信息保护法》三部网络监管“基本法”为核心依据，严格要求生成式AI技术提供者在网络安全、内容合规和个人信息保护方面的责任，反对技术滥用。

《办法》中第三条表示，“国家支持人工智能算法、框架等基础技术的自主创新、推广应用、国际合作，鼓励优先采用安全可信的软件、工具、计算和数据资源。”在明确生成式AI产品服务提供者的责任和义务方面，值得注意的是，《办法》强化了对个人信息保护的要求，比如第四条提到，“禁止非法获取、披露、利用个人信息和隐私、商业秘密”；第七条指出，“用于生成式人工智能产品的预训练、优化训练数据”，应满足“数据包含个人信息的，应当征得个人信息主体同意或者符合法律、行政法规规定的其他情形”；第十一条明确“提供者在提供服务过程中，对用户的输入信息和使用记录承担保护义务。不得非法留存能够推断出用户身份的输入信息，不得根据用户输入信息和使用情况进行画像，不得向他人提供用户输入信息。”第十三条指出，“提供者应当建立用户投诉接收处理机制，及时处置个人关于更正、删除、屏蔽其个人信息的请求。”

生成式AI迅猛发展，各国监管部门纷纷出手规范发展。 视觉中国/图

上海人工智能研究院副总工程师沈灏认为，《办法》体现了监管部门对生成式AI的一个有限范围的小心求证过程，保障在还不清楚生成式AI的各种可能性之前，各方安全可控地进行研发。

对企业影响：安全合规成本增加

“如何在规范保障网络信息安全的同时，鼓励推动相关产业发展、发挥新技术的商业及社会价值，还需要监管方面进一步探讨与平衡。”

最近一个月，包括百度、360、阿里巴巴、商汤科技、华为、科大讯飞等一众科技企业纷纷展示或即将推出AI大模型及相关应用产品，围绕生成式AI的创业热潮汹涌，国产AI大模型混战开启。

一位AI领域资深专家告诉记者，《办法》将主要从三个方面对相关企业产生影响，加大安全合规的成本。首先，其第七条要求“提供者应当对生成式人工智能产品的预训练数据、优化训练数据来源的合法性负责”，那么企业预训练的数据来源要合规、不能侵犯知识产权等，保证数据真实性、准确性等，显然是增大了企业的数据获取筛选成本；第二，提供生成式AI产品或服务应遵守法律法规、尊重社会公德公序良俗，在训练时要解决“人机对齐”问题，安全评估如果不通过需要在三个月内整改，对企业来说合规的压力加大；第三，企业还需要制定人工标注规则、对标注人员进行培训等，接受抽样检验、申报安全评估及备案等，以及第二十条规定的处罚措施，如“拒不改正或情节严重的，责令暂停或终止，并处以一万元以上十万元以下罚款”等，都会增大企业的安全合规压力及成本。

夏海龙则指出，《办法》内容最值得企业关注、或许也最容易引起业界争议的是第五条，该条规定生成式人工智能产品提供者需要对其产品生成内容承担内容生产者责任，这一规定背后的逻辑似乎认为生成式人工智能产品生成的内容完全由其开发者、设计者决定，显然这一理解与目前业界普遍看法或期待存在一定的差异，目前关于生成式AI是否具有著作权以及著作权归属、生成式人工智能对人类职业的冲击等社会讨论逐渐活跃，尚无定论，还需要进一步探讨研究。所以，如何在规范保障网络信息安全的同时，鼓励推动相关产业发展、发挥新技术的商业及社会价值，还需要监管方面进一步探讨与平衡。

在盘和林看来，《办法》目前还处在征求意见阶段，未来必然还会有相应的调整。其部分内容还需要进一步细分优化，如AI生成内容真实准确性如何界定、AI算法安全评估标准如何制定等。他认为“先规范、再发展是正确的思路”，在给AI发展戴上“紧箍”同时要尽可能地将红线划细，“红线越细，企业发展的空间才会越大”。当前，国内还没有生成式AI产品面向公众真正开放，因此在规范的同时，建议采用适当举措鼓励产业发展。从经济学角度，要警惕出现两种情况，一是正规的生成式AI厂商不敢投入研发——担忧研发后遇到风险，二是非正规产品或趁机占据市场需求的空白。因此，建议监管部门在未来持续完善相关的法律法规，丰富管理措施。

生成式AI加持 SaaS服务商将迎新生？

本报记者 曲忠芳 李正豪 北京报道

近期，由ChatGPT引发的生成式AI新浪潮给社会经济生活带来了持续的冲击与影响。如何顺应技术趋势，抓住发展机遇，成为摆在每个行业企业面前的考验与挑战，而对于自身“造血”能力尚不成熟的SaaS（软件运营服务）服务商来说显得更加迫切。

《中国经营报》记者从多家SaaS企业了解到，许多公司在内部组织架构管理方面都做了一些调整，向AI技术及相关人才方向倾斜，探索挖掘AI+SaaS的新价值及新模式；与此同时，在外部不断加大与AI技术公司的生态合作，密切关注生成式AI的商业化机遇。

华西证券最新研报指出，从海外GPT大模型应用的实践来看，AI生成内容（AIGC）在数字营销、文档、图片、游戏、影视领域已有较为成熟的应用；MaaS（模型即服务）模式赋能B端客户服务、数据分析、安全等场景，应用于金融、营销、互联网等领域。另据高盛首席软件分析师Kash Rangan团队发布的报告分析，AI浪潮将成为全球生产力的重要推手，未来十年，全球每年生产力的提升将推动7万亿美元的经济增长。现有的软件服务产业，也将因融合生成式AI的附加功能而产生一定的增值空间。

探索业务增长新路径

“AIGC是大趋势，纷享销客在今年年初已成立了专门的AIGC研究小组，该小组的主要工作在于，一是深度了解整个大模型的特征和能力，二是加强与营销智能化企业的深度交流，三是与包括百度文心一言在内的AI大模型平台进行对接，四是立足纷享销客自身的产品与业务，与用户、客户一起深度地思考在营、销、服等领域的创新，提升CRM（客户关系管理）系统的智能化水平。”纷享销客创始人兼CEO罗旭在接受记者采访时如是表示。

罗旭指出，通用AI大模型及AIGC的出现将重新定义SaaS服务，尤其是各个行业领域的SaaS与AI的结合，将加速推动SaaS从工具型、业务型向智能型、赋能型转变。在这种情况下，SaaS企业应当顺势而为，做产品及业务的创新，否则就会被颠覆。从纷享销客所在的CRM赛道来看，AIGC将大幅提升整个营销流程的生产力，例如提升营销内容的生产及创作能力和效率，更加精准地把握理解客户需求，促进交易达成；此外，AI对非结构化信息的处理能力，能够提升CRM系统的智能化程度，既从客户维度把握需求变化和客户质量，又可以洞察销售人员跟进及服务客户的有效性，给他们提供更加精准高效的赋能。

高盛研究报告显示，CRM使用生成式AI的重点将围绕三个方面，包括拥有实时可操作的数据，策划定制的销售动机，生成动态、可扩展和个性化的内容。CRM由销售、营销、服务和商务组成，生成式AI将逐步整合这一领域，并侧重根据不同数据的训练模型，来产生建议、内容、分析和结果。下一步的演变可能是定制策划方案并销售，通过利用现有的客户相关数据和对以往工作的洞察力，生成式AI可以提出经过验证的策略，并与客户产生更多的共鸣，提高效率，同时维护公司的品牌形象。最后，公司有可能利用这项技术，通过利用客户的数据，如电子邮件、手机等，创建个性化、动态、可扩展的内容。

除了纷享销客等CRM服务商之外，4月12日在港交所挂牌上市的HRSaaS平台北森控股（09669.HK），早在今年3月初就宣布成为百度文心一言的首批生态合作伙伴，将借助AI技术实现在招聘面试、员工问题解决等场景中的升级。

通讯服务商容联云AI研究院院长刘杰告诉记者，ChatGPT所代表的大语言模型，为智能客服相关技术的进一步突破带来了新的方向。一方面，ChatGPT在人机对话方面的能力，有助于提升智能客服对话的自然性，能更好地理解用户的问题，从而进一步拉升产品的用户体验；另一方面，ChatGPT的用途不仅限于人机对话，也能完成写文章、统计表格、制定方案等复杂的AI任务，这种智力行为背后采用的AIGC关键技术，也将为智能客服带来智能化的提升。

各行业企业开始探索挖掘AI+的新价值及新模式。 视觉中国/图

微盟则在公告中展望2023年业务时提到，积极跟进AI等新技术方向，探求应用层机遇。微软方面认为，GPT等人工智能新技术的出现对其所在的行业会有极大的推动和升级，相信这些新技术在应用层存在很多的可能与机遇。在零售场景中，该公司已经在广告与营销、数据智能、运营提效、用户体验等领域有初步的技术应用规划和产品端的探索，有关技术应用和产品未来落地将能助力商家智慧经营、效率提升。

SaaS困局能否破解？

毫无疑问，在生成式AI的发展浪潮下，SaaS服务商争相向AI相关技术及领域加码布局，探索新的业务可能性和增长空间。AI+SaaS，抑或是SaaS+AI，屡屡被业界提及并使用。

值得一提的是，就在今年3月中旬，金沙江创投主管合伙人朱啸虎在公开发言中表示，“过去几年里，投资人对企业服务的增长率特别失望”，他认为“中国企服的春天可能需要等5至10年”，而“最近GPT-4出来后，企服的寒冬可能漫漫无期”。由此在SaaS产业界、投资圈中引发了不小的争议与讨论。

多位SaaS从业人士向记者表达了各自的看法，他们坦言企服业务、SaaS模式在国内市场仍处在一个较早期的阶段，市场渗透的深度及广度仍有待开拓。谈及ChatGPT引领的AI新浪潮，多数受访者认为，“漫漫寒冬”说法过于悲观，这是因为当前出现的大模型仍然有缺陷，仍需要数据的训练，对于SaaS企业来说，服务的需求还在，只不过产品及业务的模式、形态可能会发生改变。对于SaaS企业来说，AI技术手段已然成为刚需，即通过对数据的流转整合实现对业务层面的智能加持，随着AI技术的逐渐成熟，SaaS企业的人工智能能力已经成为标配，甚至可以说是入场的门槛。

罗旭表示，“纷享销客并没有利用热潮去炒噱头、投机取巧，当下的工作重点还是研究了解大模型的特性及能力，基于自身营销服一体化的战略布局，以及在客户销售管理更加智能化的目标指引下，持续做长周期的建设，成长为更加智能的CRM，这将是一次质的飞跃。”

同样，金蝶中国总裁章勇也公开表示，ChatGPT在人工智能领域是重要的里程碑，它拥有非常强的学习和成长能力，未来可嵌入企业的很多场景，能全年无休地帮助企业处理基础性、重复性工作。相信随着ChatGPT的深入应用，未来在整个系统里面，会对我们的产品形成大的颠覆，让我们变得更加开放，连接到我们想要的任何地方，这十分值得期待。

高盛研究报告预计SaaS公司与AI企业将进行合作，而非竞争关系，那些成功利用生成式AI的SaaS公司将有望获得上市机会。这是因为，将AI与B2B SaaS解决方案结合起来，有望增强技术护城河，SaaS公司拥有大量客户、人力资源、财务、医疗等数据，通过数据来加强和训练人工智能驱动的大型语言模型，可以帮助SaaS公司提取关键见解、流程任务自动化，同时也能提高员工效率。